

AMENDMENT TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 1. (Currently Amended) A method of securely communicating information in a network that
2 includes a host that originates a request, a first server that serves a response to the request,
3 and a second server that cooperates with the first server to respond to the request, the
4 method comprising the computer-implemented steps of:

5 receiving a first request for a service from the host by the first server, which request

6 includes a network address of the host; ~~and~~

7 comparing a network address of the first server to a network address of the second

8 server to determine if the network address of the first server is identical to the

9 network address of the second server; and

10 if the network address of the first server is determined to be identical to the network

11 address of the second server, communicating a second service request from

12 the first server to the second server when the first service request includes

13 functions not available in the first server, said second service request

14 including the host network address ~~only when a first network address of the~~

15 ~~first server is identical to a second network address of the second server.~~

1 2. (Currently Amended) A method as recited in Claim 1, wherein the first request of from the
2 host comprises a key value comprising an originating host Internet Protocol (IP) address and
3 a random value.

1 3. (Currently Amended) A method as recited in Claim 1, wherein the step of comparing a
2 network address of the first server to a network address of the second server to determine if
3 they are identical ~~communicating a second service request~~ comprises the step of accepting

4 ~~the host request only when comparing~~ an IP address of the second server ~~is the same as to an~~
5 IP address of the first server.

1 4. (Original) A method as recited in Claim 1, wherein the host is a Web browser and wherein
2 the host request comprises a Universal Resource Locator (URL) that includes an IP address
3 of the host.

1 5. (Original) A method as recited in Claim 1, wherein the host is a Web browser and wherein
2 the host request comprises an HTML POST form that includes an IP address of the host.

1 6. (Currently Amended) A method of securely communicating data between a proxy server
2 and a second server, wherein each of the proxy server and the second server are addressable
3 by first and second Internet Protocol (IP) addresses, respectively, the method comprising the
4 computer-implemented steps of:

5 receiving, at the proxy server, a first service request from a browser client, wherein
6 the service request includes a third IP address of a client computer associated
7 with the browser client;

8 comparing the first IP address of the proxy server to the second IP address of the
9 second server to determine if they are identical; and

10 communicating a second service request that includes the browser client IP address
11 from the proxy server to the second server only when the first IP address of
12 the proxy server is determined to be identical to the second IP address of the
13 second server.

1 7. (Original) A method as recited in Claim 6, wherein the first service request of the browser
2 client comprises a key value comprising the third IP address and a random value.

1 8. (Currently Amended) A method as recited in Claim 6, wherein the first service request of
2 the browser client comprises a Universal Resource Locator (URL) that includes an IP address
3 of the ~~host~~ client computer associated with the browser client.

1 9. (Currently Amended) A method as recited in Claim 6, wherein the first service request of
2 the browser client comprises an HTML POST form that includes an IP address of the ~~host~~
3 client computer associated with the browser client.

1 10. (Currently Amended) A method of securely communicating a network address of a client
2 that issues service requests to a first server that proxies the service requests for a second
3 server, comprising the computer-implemented steps of:
4 receiving a network address of the client by the first server;
5 determining whether a first network address of the first server is equal to a second
6 network address of the second server; and
7 sending the network address of the client from the first server to the second server in
8 a secure request message only when the first network address of the first
9 server is equal to the second network address of the second server.

1 11. (Currently Amended) A method as recited in Claim 10, wherein each of the service
2 requests of the ~~browser~~-client comprises a key value comprising an IP address of the client
3 and a random value.

1 12. (Currently Amended) A method as recited in Claim 10, wherein each of the service
2 requests of the ~~browser~~ client comprises a Universal Resource Locator (URL) that includes
3 an IP address of the ~~browser~~ client.

1 13. (Currently Amended) A method as recited in Claim 10, wherein each of the service
2 requests of the ~~browser~~ client comprises an HTML POST form that includes an IP address of
3 the ~~browser~~ client.

1 14. (Currently Amended) A data communications apparatus that securely communicates a
2 service request that is received from a client, comprising a first server that receives the
3 service request from the client, proxies the service request for a second server, the first server

comprising means for receiving a network address of the client; means for determining whether a first network address of the first server is equal to a second network address of the second server; and means for sending the network address of the client from the first server to the second server in a secure request message only when the first network address of the first server is equal to the second network address of the second server.

15. (Original) An apparatus as recited in Claim 14, wherein the service request comprises a key value comprising an IP address of the client and a random value.

16. (Currently Amended) An apparatus as recited in Claim 14, wherein the service request comprises a Universal Resource Locator (URL) that includes an IP address of the ~~browser~~ client.

17. (Currently Amended) An apparatus as recited in Claim 14, wherein the service request comprises an HTML POST form that includes an IP address of the ~~browser~~ client.

18. (Currently Amended) A computer-readable medium carrying one or more sequences of instructions for securely communicating a network address of a client that issues service requests to a first server that proxies the service requests for a second server, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

receiving a network address of the client by the first server;

determining whether a first network address of the first server is equal to a second network address of the second server; and

sending the network address of the client from the first server to the second server in a secure request message only when the first network address of the first server is equal to the second network address of the second server.

1 19. (Currently Amended) A computer-readable medium as recited in Claim 18, wherein each
2 of the service requests of the ~~browser~~ client comprises a key value comprising an IP address
3 of the client and a random value.

1 20. (Currently Amended) A computer-readable medium as recited in Claim 18, wherein each
2 of the service requests of the ~~browser~~ client comprises a Universal Resource Locator (URL)
3 that includes an IP address of the ~~browser~~ client.

1 21. (Currently Amended) A computer-readable medium as recited in Claim 18, wherein each
2 of the service requests of the ~~browser~~ client comprises an HTML POST form that includes an
3 IP address of the ~~browser~~ client.

1 22. (Original) A data communications apparatus that securely communicates a service
2 request that is received from a client, comprising:
3 a first server that proxies the service request for a second server comprising a network
4 interface to a network that includes the first server and the second server;
5 a processor in the first server;
6 a storage device in the first server comprising one or more sequences of stored
7 instructions which, when executed by the processor, cause the processor to
8 carry out the steps of:
9 receiving a network address of the client;
10 determining whether a first network address of the first server is equal to a
11 second network address of the second server; and
12 sending the network address of the client from the first server to the second
13 server in a secure request message only when the first network address of the
14 first server is equal to the second network address of the second server.

1 23. (Original) An apparatus as recited in Claim 22, wherein the service request comprises a
2 key value comprising an IP address of the client and a random value.

1 24. (Currently Amended) An apparatus as recited in Claim 22, wherein the service request
2 comprises a Universal Resource Locator (URL) that includes an IP address of the ~~browser~~
3 client.

1 25. (Currently Amended) An apparatus as recited in Claim 22, wherein the service request
2 comprises an HTML POST form that includes an IP address of the ~~browser~~ client.